Rev. 01/2015

STATE OF SOUTH DAKOTA
OFFICE OF PROCUREMENT MANAGEMENT
523 EAST CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501-3182

1094/1095 B IRS FORM DISTRIBUTION/TRANSMISSION

PROPOSALS ARE DUE NO LATER THAN September 18th, 2015, 5:00 pm CDT

RFP #359

BUYER: Department of Social Services, Division of Economic Assistance

POC: Mark Close
Mark.Close@state.sd.us

READ CAREFULLY

FIRM NAME: ______________________ AUTHORIZED SIGNATURE: ______________

ADDRESS: ______________________ TYPE OR PRINT NAME: ______________

CITY/STATE: ______________________ TELEPHONE NO: ______________________

ZIP (9 DIGIT): ______________________ FAX NO: ______________________

FEDERAL TAX ID#: __________________ E-MAIL: ______________________

PRIMARY CONTACT INFORMATION

CONTACT NAME: ______________________ TELEPHONE NO: ______________________

FAX NO: ______________________ E-MAIL: ______________________

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

In March 2010, Congress passed two pieces of legislation that the President later signed into law – the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act. The Health Care and Education Reconciliation Act of 2010 (HCERA) and the Patient Protection and Affordable Care Act (PPACA) are collectively referred to as the Affordable Care Act (ACA).

The Internal Revenue Service (IRS) is responsible for implementing major portions of the Patient Protection and Affordable Care Act (PPACA), commonly referred to as the Affordable Care Act or ACA. The ACA Information Returns (AIR) Project is responsible for delivering applications, infrastructure, and supporting processes required to process information returns. In October 2015, AIR will begin processing Tax Year (TY) 2014 Forms 1094/1095-B and Forms 1094/1095-C; TY 2014 is voluntary. In January 2016, TY 2015 Forms 1094/1095-B and Forms 1094/1095-C will be mandatory.

As part of this law, insurers and certain employers are required to file these new information returns with the Internal Revenue Service. The IRS will receive and process these information returns. Forms will also need to be sent to individuals that received MEC (Minimum Essential Coverage) during the tax year.

Due to complexities in the make-up of Medicaid Households and the changes that occur through-out the year, the State of South Dakota expects to send one 1095 B form for each recipient. The forms will be sent to the current address on record for each recipient.

The State of South Dakota is seeking a vendor to provide the technical and operational services required to:

1. Generate 1095-B forms and mail them to all Medicaid and CHIP recipients in South Dakota that meet the Affordable Care Act definition of having had MEC during the previous calendar year such that recipients receive the form no later than January 31 of each year, starting in January 2016.

2. Generate a file for transmission to IRS no later than March 31st of each year (with subsequent transmissions on a monthly basis after that date) that contains the data required by IRS specifications for 1094 A and 1095 B processing, starting in March 2016.

The State is looking for a service vendor that can perform this service after receipt of a file from the State of all recipients who had eligibility during any month(s) for the previous tax year, starting with Tax Year 2015. The State is looking for a vendor to support this process for a minimum of three (3) years starting with processing of Tax year 2015, with an option to extend for an additional year(s).

The State of South Dakota intends to use this service for Medicaid reporting but may expand the use of the service to address other current or future ACA requirements.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Department of Social Services, Division of Economic Assistance is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Social Services, Division of Economic Assistance. The reference number for the transaction is RFP #359. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

Please refer to the Department of Social Services website link http://dss.sd.gov/keyresources/rfp.aspx for the RFP, any related questions/answers, changes to schedule of activities, amendments, etc.

1.3 LETTER OF INTENT

All interested offerors are requested to submit a non-binding **Letter of Intent via email to the point of contact, Mark Close, at mark.close@state.sd.us,** to respond to this RFP. **While preferred, a Letter of Intent is not mandatory to submit a proposal**.

The letter of intent must be received in the Department of Social Services by no later than September 1st . Place the following in the subject line of your email: "Letter of Intent for RFP #359." Be sure to reference the RFP number in any attached letter or document.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	August 17, 2015
Letter of Intent to Respond Due	September 1, 2015
Deadline for Submission of Written Inquiries	September 1, 2015
Responses to Offeror Questions	September 4, 2015
Proposal Submission	September 18, 2015, 5:00 pm, CDT
Oral Presentations/discussions (if required)	TBD
Anticipated Award Decision/Contract Negotiation	September 25, 2015

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the Department of Social Services, Division of Economic Assistance by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be late and ineligible for consideration.

An original, 5 identical copies, and one (1) digital copy of the proposal shall be submitted.

All proposals must be signed in ink by an officer of the responder legally authorized to bind the responder to the proposal, and sealed in the form intended by the respondent. Proposals that are not properly signed may be rejected. The sealed envelope must be marked with the appropriate RFP Number and Title. The words "Sealed Proposal Enclosed" must be prominently denoted on the outside of the shipping container. **Proposals must be addressed and labeled as follows:**

Request For Proposal #359 Proposal Due September 18, 2015
South Dakota Department of Social Services
Attention: Mark Close
700 Governors Drive
Pierre SD 57501-2291

No punctuation is used in the address. The above address as displayed should be the only information in the address field.

No proposal may be accepted from, or any contract or purchase order awarded to any person, firm or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

1.6 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the bidder shall attach an explanation to their offer.

1.7 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.8 MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.9 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after September 1, 2015. Email inquiries must be sent to Mark Close (mark.close@state.sd.us) with the subject line "RFP #359."

The Department of Social Services will respond to offerors inquiries by posting the offeror aggregated questions and Department responses on the DSS website at http://dss.sd.gov/keyresources/rfp.aspx no later than September 4, 2015. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.10 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information. Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. Pricing and service elements are not considered proprietary. An entire proposal may not be marked as proprietary. Offerors must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

1.11 LENGTH OF CONTRACT

The solution presented in the vendor responses shall cover a contract period of three (3) years with option for an additional year(s).

1.12 GOVERNING LAW

Venue for any and all legal action regarding or arising out of the transaction covered herein shall be solely in Hughes County, State of South Dakota. The laws of South Dakota shall govern this transaction.

1.13 DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

An oral presentation by an offeror to clarify a proposal may be required at the sole discretion of the State. However, the State may award a contract based on the initial proposals received without discussion with the offeror. If oral presentations are required, they will be scheduled after the submission of proposals. Oral presentations will be made at the offeror's expense.

This process is a Request for Proposal/Competitive Negotiation process. Each Proposal shall be evaluated, and each respondent shall be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any and/or all components of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2.0 STANDARD AGREEMENT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State's standard terms and conditions as seen in Attachment A.

3.0 SCOPE OF WORK

Proposals must provide a description for each of the following requirements of how the requirements will be met.

3.1 The State of South Dakota is requesting that respondents have a service for submitting/distributing forms 1094/1095 B, that is currently developed or will be developed for the optional tax year 2014 submission deadline. The vendor's solution must adhere to IRS Publications 5164 and 5165. The vendor must adhere to all IRS requirements for successfully submitting files through the AIR (Affordable Care Act (ACA) Information Returns) application.

3.2 The State of South Dakota will create a file containing the individuals that received Minimum Essential Coverage for Medicaid or CHIP for the prior tax year. The file will contain all data elements currently outlined in the 1095 B Schema to form a crosswalk. This file will be in a mutually agreed upon format for the vendor to use when creating the 1095 B forms and the electronic transactions with the IRS. Provide a description of the process of sending a file to ensure Personally Identifiable Information (PII) is handled in a secure manner.

3.3 The selected vendor will be responsible for submitting the file to the IRS in the approved .xml format prior to the applicable IRS deadlines. Alternatively, the vendor can provide an equivalent process for submitting the proper file to the AIR application**.**

3.4 The selected vendor will be responsible for distributing the 1095 B forms to the South Dakota Medicaid recipients prior the applicable IRS deadlines. Alternatively, the vendor can provide an equivalent process for distributing the 1095 B forms to recipients. The vendor should allow for bundling of forms that go to the same household. There are approximately 119,000 active South Dakota Medicaid recipients. Due to recipients going on and off Medicaid throughout the year, the number of transactions and paper forms distributed will be higher**.**

3.5 Throughout the year there may be changes to the SD Medicaid recipients' eligibility, either the addition of retroactive eligibility or removal of eligibility. The selected vendor will be responsible for submitting the file for changes that occur through-out the year to the IRS in the approved .xml format. The selected vendor will also be responsible for distributing 1095 B forms for changes that occur through-out the year to South Dakota Medicaid recipients.

3.6 The selected vendor will provide functionality for the State of South Dakota to be able to perform a check to verify the 1095 B forms are being generated accurately. The State of South Dakota should also have functionality to approve the distribution of the forms to either the IRS or recipients.

3.7 Provide a detailed description for performing testing. Including State-to-vendor testing and State-to-vendor-to IRS-testing.

3.8 Provide functionality to resend specific 1095 B forms to recipients upon request. Allow the State to resend corrected 1095 B forms to replace forms that contained incorrect information. Alternatively, the vendor can provide a service that would allow the vendor to resend replacement 1095 B forms to recipients.

3.9 Provide functionality for approximately 50 role-based users to login to the application simultaneously to perform work, including; reporting, resending corrected 1095 B forms, investigating forms that were not received by recipients, etc.

3.10 Provide functionality to allow the use of an alternative recipient identifier to facilitate searching for recipients with no SSN.

3.11 The selected vendor will be responsible for reprocessing any transaction errors and notifying the State of South Dakota in a timely manner.

3.12 Provide functionality for the State of South Dakota to perform reporting such as: number of recipients' information sent to the IRS over a specific time period, number of 1095 B forms resent over a specific time period, transaction errors, etc. Provide functionality to allow ad-hoc reporting.

3.13 To ensure business continuity, provide a plan for business continuity and disaster recovery to enable the State to continue to meet the IRS requirements of IRS 1095 processing.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

4.2 Offeror's Contacts: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to the point of contact of the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the buyer of record.

4.3 The offeror May be required to submit a copy of their most recent independently audited financial statements.

4.4 Provide the following information related to at least three previous and current service/contracts performed by the offeror's organization which are similar to the requirements of this RFP. Provide this information for any service/contract that has been terminated, expired or not renewed in the past three years:

4.4.1 Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;

4.4.2 Dates of the service/contract; and

4.4.3 A brief, written description of the specific prior services performed and requirements thereof.

4.5 While it is not anticipated, the selected vendor should be available to travel to Pierre, SD at least once per year.

4.6 The offeror must detail examples that document their ability and proven history in handling special project constraints.

4.7 If an offeror's proposal is not accepted by the State, the proposal will not be reviewed/evaluated.

4.8 Offeror must answer, sign, and submit Attachment B with their proposal, and review and acknowledge that Attachment C must be signed at contract signature.

4.9 Submit examples of prior projects to demonstrate past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration.

4.10 Identify staff that will be working on the project to ensure sufficient resources.

4.11 Describe your ability and proven history in handling special project constraints.

4.12 Describe your proposed project management techniques.

4.13 Describe your familiarity and availability with the project locale.

5.0 PROPOSAL RESPONSE FORMAT

5.1 An original and 5 copies shall be submitted.

5.1.1 In addition, the offeror must provide one (1) copy of their entire proposal, including all attachments and cost proposal, in PDF electronic format. Offerors may not send the electronically formatted copy of their proposal via email.

5.1.2 The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number.

5.2 All proposals must be organized and tabbed with labels for the following headings:

5.2.1 **RFP Form**. The State's Request for Proposal form completed and signed.

5.2.2 **Executive Summary.** The one or two page executive summary is to briefly describe the offeror's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the offeror. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests should be identified in this section.

5.2.3 **Detailed Response.** This section should constitute the major portion of the proposal and must contain at least the following information:

5.2.3.1 A complete narrative of the offeror's assessment of the work to be performed, the offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.

5.2.3.2 A specific point-by-point response, in the order listed, to each requirement in the RFP as detailed in Sections 3 and 4. The response should identify each requirement being addressed as enumerated in the RFP.

5.2.3.3 A clear description of any options or alternatives proposed.

5.2.4 **Cost Proposal.** Cost will be evaluated independently from the technical proposal. Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

The cost proposal must be submitted in a separate sealed envelope labeled "Cost Proposal".

See section 7.0 for more information related to the cost proposal.

6.0 PROPOSAL EVALUATION AND AWARD PROCESS

6.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria listed in order of importance:

6.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;
6.1.2 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;
6.1.3 Cost proposal;
6.1.4 Resources available to perform the work, including any specialized services, within the specified time limits for the project;
6.1.5 Ability and proven history in handling special project constraints;
6.1.6 Proposed project management techniques
6.1.7 Familiarity with the project locale;
6.1.8 Availability to the project locale;

6.2 Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

6.3 The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

6.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

6.5 **Award:** The requesting agency and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

6.5.1 If the agency and the highest ranked offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the contractor. The agency may then negotiate with the next highest ranked contractor.

6.5.2 The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached or the agency terminates the contracting process.

7.0 **COST PROPOSAL**

When submitting cost proposals, if there are multiple options, prepare a cost proposal for each option and the services covered. Provide costs for all services provided plus any yearly maintenance, training and one-time set-up costs.

The cost proposal shall cover a contract period of three (3) years with the option for an additional year(s). The proposal shall cover all fixed costs, to include maintenance and operations, over that time period. If there are additional per member costs, those need to be covered independently.

The Cost proposal should be submitted in a separate, sealed envelope and clearly marked with Vendor Name, Response to SD 1095 Processing and Transmission RFP # 359.

Vendors should provide the following completed Cost Template for the three contract years:

Category	Contract year 1 Costs (10/01/15 – 06/30/16	Year 2 (7/01/16 – 06/30/17)	Year 3 (7/01/17 – 06/30/18)	Comments
Technical Software License Fee (if any)				
Operational Fee (mailing letters)				
Training (year 1 only)				
Initial setup fee (Year 1 only)				

Training Costs should only be listed for the first year of the contract.

Please note any clarifying comments in the Comments Column.

ATTACHMENT A

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
DIVISION OF ECONOMIC ASSISTANCE

Consultant Contract
For Consultant Services
Between

State of South Dakota
Department of Social Services
Division of Economic Assistance
700 Governors Drive
Pierre, SD 57501-2291

Referred to as Consultant	Referred to as State

The State hereby enters into a contract for consultant services with the Consultant. While performing services hereunder, Consultant is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

1. CONSULTANT'S South Dakota Vendor Number is _____________.

2. PERIOD OF PERFORMANCE:
   A. This Agreement shall be effective as of Month/Day 2015 and shall end on Month/Day 2016, unless sooner terminated pursuant to the terms hereof.

   B. Agreement is the result of Request for Proposal #___________.

3. PROVISIONS:

   A. The Purpose of this Consultant contract:
      1.

      2. Does this agreement involve Protected Health Information (PHI)? YES ( ) NO ( )

         If PHI is involved, a Business Associate Agreement must be attached and is fully incorporated herein as part of the agreement (refer to attachment _____).

      3. The consultant will/will not use state equipment, supplies or facilities.

   B. The Consultant agrees to perform the following services (add an attachment if needed.):
      1.

C. The State agrees to:

1.

2. Make payment for services upon satisfactory completion of services and receipt of bill. Payment will be in accordance with SDCL 5-26.

3. Will the State pay Consultant expenses as a separate item?

YES ( ) NO ( )

If YES, expenses submitted will be reimbursed as identified in this agreement.

D. The TOTAL CONTRACT AMOUNT will not exceed **$_____________.**

4. BILLING:
Consultant agrees to submit a bill for services within (30) days following the month in which services were provided. Consultant will prepare and submit a monthly bill for services. Consultant agrees to submit a final bill within 45 days of the contract end date to receive payment for completed services. If a final bill cannot be submitted in 45 days, then a written request for extension of time and explanation must be provided to the State.

5. TECHNICAL ASSISTANCE:
The State agrees to provide technical assistance regarding Department of Social Services rules, regulations and policies to the Consultant and to assist in the correction of problem areas identified by the State's monitoring activities

6. LICENSING AND STANDARD COMPLIANCE:
The Consultant agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this agreement. The Consultant will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Consultant's failure to ensure the safety of all individuals served is assumed entirely by the Consultant.

7. ASSURANCE REQUIREMENTS:
The Consultant agrees to abide by all applicable provisions of the following assurances: Lobbying Activity, Byrd Anti Lobbing Amendment (31 USC 1352), Debarment and Suspension, Debarment and Suspension (Executive orders 12549 and 12689),Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Americans with Disabilities Act of 1990, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013 and American Recovery and Reinvestment Act of 2009 as applicable.

8. RETENTION AND INSPECTION OF RECORDS:

The Consultant agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the program, including records and documents regarding applications, determination of eligibility (when applicable), the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State. The Consultant shall retain such records for a period of six years from the date of submission of the final expenditure report. If such records are under pending audit, the Consultant agrees to hold such records for a longer period upon notification from the State. The State, through any authorized representative, will have access to and the right to examine and copy all records, books, papers or documents related to services rendered under this Agreement. State Proprietary Information retained in Consultant's secondary and backup systems will remain fully subject to the obligations of confidentiality stated herein until such information is erased or destroyed in accordance with Consultant's established record retention policies.

All payments to the Consultant by the State are subject to site review and audit as prescribed and carried out by the State. Any over payment of this contract shall be returned to the State within thirty days after written notification to the Consultant.

9. WORK PRODUCT:
Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, State Proprietary Information, State Data, End User Data, Personal Health Information, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Contract shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.
Paper, reports, forms software programs, source code(s) and other materials which are a part of the work under this Contract will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State none the less reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

Consultant agrees to return all information received from the State to State's custody upon the end of the term of this contract, unless otherwise agreed in a writing signed by both parties.

10. TERMINATION:
This Agreement may be terminated by the State upon thirty (30) days written notice. This agreement may be terminated by the Vendor for cause with the cause explained by the Vendor in writing and upon one hundred and eighty (180) days written notice. The Vendor is obligated to give the State one hundred and eighty (180) days written notice in the event the Vendor intends not to renew the contract or intends to raise any fees or costs associated with the Vendor's products or services in a subsequent contract unless such fees or costs have previously been negotiated and included in this contract. In the event the Vendor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time with or without notice. Upon notice of termination of a contract or upon reaching the end of the term of this contract unless the contract is renewed, the State of South Dakota requires that State applications that store information to repositories not hosted on the State's infrastructure require the vendor before termination (whether initiated by the State or the Vendor) to extract the State's information such that the State is able to be load the information onto\into repositories listed in the State's Standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. Upon the effective date of the termination of the agreement the State of South Dakota again requires that State applications that store information to repositories not hosted on the State's infrastructure require the vendor before termination (whether initiated by the State or the Vendor) to extract the State's information such that the state is able to load the information onto or into repositories listed in the State's Standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. If termination for such a default is effected by the State, any payments due to Vendor at the time of termination may be adjusted to

cover any additional costs to the State because of Vendor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. In the event of termination or at the end of the term of this contract unless the contract is renewed, the Vendor shall deliver to the State all reports, plans, specifications, technical data, and all other information completed prior to the date of termination. If after the State terminates for a default by Vendor it is determined that Vendor was not at fault, then the Vendor shall be paid for eligible services rendered and expenses incurred up to the date of termination. The terms of this provision were arrived at after negotiation between the parties. This provision is the joint product or work of the parties, and not a provision written or demanded by any one party to this agreement. The Vendor recognizes and agrees, however, that the State of South Dakota cannot enter into an agreement providing for hosting of any of its data on the Vendor's servers and networks without provisions protecting its ability to access and recover its data in a usable, non-proprietary format in the event of termination of this contract with sufficient time to convert that data and the business functions provided by the Vendor to another system and vendor.

11. FUNDING:
This Contract depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of the law or federal funds reduction, this Contract will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

12. AMENDMENTS:
This Contract may not be assigned without the express prior written consent of the State. This Contract may not be amended except in writing, which writing shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

13. CONTROLLING LAW:
This Contract shall be governed by and construed in accordance with the laws of the State of South Dakota. Venue for any lawsuit pertaining to or affecting this Agreement shall be resolved in the Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

14. SUPERCESSION:
All prior discussions, communications and representations concerning the subject matter of this Contract are superseded by the terms of this Contract, and except as specifically provided herein, this Contract constitutes the entire agreement with respect to the subject matter hereof.

15. IT STANDARDS:
Consultant warrants that the software and hardware developed or purchased for the state will be in compliance with the BIT Standards including but not limited to the standards for security, file naming conventions, executable module names, Job Control Language, systems software, and systems software release levels, temporary work areas, executable program size, forms management, network access, tape management, hosting requirements, administrative controls, and job stream procedures prior to the installation and acceptance of the final project. BIT standards can be found at http://bit.sd.gov/standards/.

16. SEVERABILITY:
In the event that any provision of this Contract shall be held unenforceable or invalid by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision of this contract, which shall remain in full force and effect.

17. NOTICE:
Any notice or other communication required under this Contract shall be in writing and sent to the address set forth above. Notices shall be given by and to the Division being contracted with on behalf of the State, and by the Consultant, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

18. SUBCONTRACTORS:
The Consultant may not use subcontractors to perform the services described herein without express prior written consent from the State. The State reserves the right to reject any person from the contract presenting insufficient skills or inappropriate behavior.

The Consultant will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Contract, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Contract. The Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Consultant is required to assist in this process as needed.

19. HOLD HARMLESS:
The Consultant agrees to hold harmless and indemnify the State of South Dakota, its officers, agents and employees, from and against any and all actions, suits, damages, liability or other proceedings which may arise as the result of performing services hereunder. This section does not require the Consultant to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

20. INSURANCE:
Before beginning work under this Contract, Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Contract. The Consultant, at all times during the term of this Contract, shall obtain and maintain in force insurance coverage of the types and with the limits listed below. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Consultant agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Consultant shall furnish copies of insurance policies if requested by the State.

A. Commercial General Liability Insurance:
Consultant shall maintain occurrence-based commercial general liability insurance or an equivalent form with a limit of not less than $1,000,000 for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Contract or be no less than two times the occurrence limit.

B. Business Automobile Liability Insurance:
Consultant shall maintain business automobile liability insurance or an equivalent form with a limit of not less than $500,000 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles.

C. Worker's Compensation Insurance:
Consultant shall procure and maintain Workers' Compensation and employers' liability insurance as required by South Dakota law.

D. Professional Liability Insurance:
Consultant agrees to procure and maintain professional liability insurance with a limit not less than $1,000,000.

(Medical Health Professional shall maintain current general professional liability insurance with a limit of not less than one million dollars for each occurrence and three million dollars in the aggregate. Such insurance shall include South Dakota state employees as additional insureds in the event a claim, lawsuit, or other proceeding is filed against a state employee as a result of the services provided pursuant to this Contract. If insurance provided by Medical Health Professional is provided on a claim made basis, then Medical Health Professional shall provide "tail" coverage for a period of five years after the termination of coverage.)

21. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:
Consultant certifies, by signing this agreement, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by the federal government or any state or local government department or agency. Consultant further agrees that it will immediately notify the State if during the term of this Contract either it or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

22. CONFLICT OF INTEREST:
Consultant agrees to establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal organizational conflict of interest, or personal gain. Any potential conflict of interest must be disclosed in writing.

23. REPORTING PROVISION:
Consultant agrees to report to the State any event encountered in the course of performance of this Contract which results in injury to any person or property, or which may otherwise subject Consultant, or the State of South Dakota or its officers, agents or employees to liability. Consultant shall report any such event to the State immediately upon discovery.
Consultant's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Consultant's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Consultant to report any event to law enforcement or other entities under the requirements of any applicable law.

24. CONFIDENTIALITY OF INFORMATION:
For the purpose of the sub-paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. Consultant acknowledges that it shall have a duty to not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. Consultant shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this contract; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this contract; (iii) make State Proprietary Information available to any of its employees, officers, agents or consultants except those who have agreed to obligations of confidentiality at least as strict as those set out in this contract and who have a need to know such information. Consultant is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. Consultant shall protect confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. State Proprietary Information shall not include information that (i) was in the public domain at the time it was disclosed to Consultant; (ii) was known to Consultant without restriction at the time of disclosure from the State; (iii) that is disclosed with the prior written approval of State's officers or employees having authority to disclose such information; (iv) was independently developed by Consultant without the benefit or influence of the State's information; (v) becomes known to Consultant without restriction from a source not connected to the State of South Dakota. State's Proprietary Information shall include names, social security numbers, employer numbers, addresses and all other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under applicable

State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6, SDCL 28-1-29, SDCL 28-1-32, and SDCL 28-1-68 as applicable federal regulation and agrees to immediately notify the State if the information is disclosure, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the contract except as required by applicable law or as necessary to carry out the terms of the contract or to enforce that party's rights under this contract. Consultant acknowledges that the State and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this contract for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Consultant will be required to undergo investigation.

25. APPLICATION OF CONTRACT TERMS
All of the following terms and provisions are applicable to each and every entity that hosts State data. If Vendor subcontracts any hosting of State data to another entity, the relationship between Vendor and any such subcontracting entity must be that of Principal and Agent. No such Agent may act as an independent contractor for Vendor. Vendor must include in its contract with any such Agent explicit terms providing for this Principal and Agent relationship, and Vendor must further supervise such Agent so as to insure that such Agent complies with all of the following terms.

26. THIRD PARTY HOSTING
If (Vendor name here) has the State's or end user's data hosted by another party (Vendor name here) must provide the State the name of this party and the terms of service, agreement or contract (Vendor name here) has with this other party. It is permissible for (Vendor name here) to redact any pricing or cost information from these documents. (Vendor name here) must provide the State with contact information for this third party and the location of their data center(s). (Vendor name here) must receive from the third party written assurances that the state and or end user data will reside in the United States at all times and provide these written assurances to the State. If the terms of service, agreement or contract as well as the location of the data center(s) and the written assurance that the data will reside in the United States is not acceptable to the State the State may terminate this contract and seek another service provider without penalty. Failure to abide by any of these terms will be considered a breach of this contract by (Vendor name here).

27. DISASTER RECOVERY
The Contractor will maintain a disaster recovery plan (the "Disaster Recovery Plan") with respect to the services provided to the State. For purposes of this Agreement, a "Disaster" shall mean any unplanned interruption of the operation of or inaccessibility to the Contractor's service in which the State, using reasonable judgment, requires relocation of processing to a recovery location. The State shall notify the Contractor as soon as possible after the State deems a service outage to be a Disaster. The Contractor shall move the processing of the State's services to a recovery location as expeditiously as possible and shall coordinate the cut-over.

28. AUDIT
When hosting any state data that may be confidential, private, financially sensitive, or contain personally identifiable information, the vendor must agree to Allow the state at the state's expense to perform up to two security audit and vulnerability assessments per year to provide verification of Vendor's IT security safeguards for the system and its data. The state will work with the Vendor to arrange the audit at a time least likely to create work load issues for the Vendor and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

The Vendor agrees to work with the state to rectify any serious security issues revealed by the security audit and vulnerability assessments. This includes additional security audits and vulnerability assessments that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. It is required that any security audits must meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS) irrespective of there being any PCI DSS data involved.

29. FACILITIES INSPECTION
The Contractor grants authorized state and/or federal personnel access to inspect their systems, facilities, work areas, contractual relationships with third parties involved in supporting any aspects of the hosted system, and the systems which support/protect the hosted system. This access will be granted on 24 hour notice. Such

personnel will be limited to staff authorized by the state or the federal government to audit the system, and representatives of the state entity that funds the hosting. The state accepts that access will be arranged with an escort, and the Contractor commits that the escort will have the access and authority to provide physical access to facilities, answer appropriate questions, and provide requested documentation, including but not limited to executed contract terms, operating procedures, records of drills and tests, evidence of background checks, security logs, and any other items required by state or federal audit requirements or as deemed by the state to be required to demonstrate the Contractor is complying with all contract terms.

30. REDUNDANT POWER AND COOLING TO ALL HARDWARE
The Contractor will provide documentation and, at the discretion of the state, allow for on-site inspections as needed to demonstrate all facilities supporting the application have adequate redundant power and cooling capacity to operate uninterrupted, and without the need to refuel generators, for not less than 24 hours in the event the local external power fails.

31. UPS BACKUP
The Contractor will provide documentation and, at the discretion of the state, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate UPS power to carry the systems for not less than 10 minutes, and to protect the system from power fluctuations including, but not limited to, surge, spikes, sags, and instability.

32. MIGRATION CAPABILITY
Upon termination or expiration of this Agreement, the Contractor will ensure that all State and End User Data is transferred to the State or a third party designated by the State securely, within a reasonable period of time, and without significant interruption in service, all as further specified in the Technical Specifications provided in the RFP. The Contractor will ensure that such migration uses facilities and methods that are compatible with the relevant systems of the transferee, and to the extent technologically feasible, that the State will have reasonable access to State and End User Data during the transition.

The Contractor will notify the State of impending cessation of its business or that of a tiered provider and any contingency plans in the event of notice of such an event. This includes immediate transfer of any previously escrowed assets and data and State access to the Contractor's facilities to remove or destroy any State-owned assets and data. The Contractor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Contractor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Contractor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Contractor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

33. HOST FACILITY PHYSICAL SECURITY
The Contractor will provide documentation and, at the discretion of the state, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate physical security. This includes, at a minimum, centrally administered electronic locks that control entry and exit from all rooms where the hosted system resides. Any door security system must either be connected to the building's power backup system as defined elsewhere or have internal battery power sufficient to last 24 hours in normal usage. Security events for the physical access system must be logged and the logs stored electronically in a secure location in a non-changeable format and must be searchable. Retention on the logs must be not less than 7 years. Log entries must be created for at least: successful entry and exit (indicating whether the access was to enter or exit the room) as well as all security related events such as, doors left open more than 30 seconds, forced entries, failed entry attempts, repeat entries without exit, repeat exits without entry, attempts to access doors for which access was not authorized. The Contractor agrees to provide, at the state's request, full access to search the security logs for any access or security events related to any and all rooms and physical locations hosting the state's system.

34. HOST NETWORK SECURITY
The Contractor will use industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement as indicated in the Information Technology User Security Guide.

The Contractor will, at its expense, either conduct or have conducted at least on an annual basis and provide to the state upon its request:

A. A vulnerability scan, performed by a scanner approved by the State, of the Contractor's systems and facilities that are used in any way to deliver services under this Agreement; and
B. A formal penetration test, performed by a process and qualified personnel approved by the State, of the Contractor's systems and facilities that are used in any way to deliver services under this Agreement.

35. LEGAL REQUESTS FOR DATA
Except as otherwise expressly prohibited by law, the Contractor will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Contractor seeking State and/or End User Data maintained by the Contractor;
B. Consult with the State regarding its response;
C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and
D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

36. EDISCOVERY
The Contractor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Contractor shall not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

37. DATA EXCHANGE AND ENCRYPTED DATA STORAGE
All facilities used to store and process State and End User data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Contractor warrants that all State and End User Data will be encrypted in transmission (including via web interface) and storage at no less than 128-bit level encryption.

38. MULTI-TENANT ARCHITECTURE LOGICALLY/PHYSICALLY SEPARATED TO INSURE DATA SECURITY
The Contractor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate safeguards to assure that needed logical and physical separation is in place and enforced to insure data security, physical security, and transport security.

39. ACCESS ATTEMPTS
All access attempts, whether failed or successful, to any system connected to the hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity shall be logged by the Contractor. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the state, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the hosted system.

40. PASSWORD POLICIES

Password policies for all Contractor employees will be documented annually and provided to the state to assure adequate password protections are in place. Logs and administrative settings will be provided to the state on request to demonstrate such policies are actively enforced.

41. SYSTEM UPGRADES
Advance notice of ___ shall be given to the State of any major upgrades or system changes that the Contractor will be implementing. A major upgrade is a replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes.

42. SEPARATION OF JOB DUTIES
The Contractor shall require commercially reasonable non-disclosure agreements, and limit staff access to State data to that which is required to perform job duties.

43. PROVISION OF SERVICES
The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided.

44. IDENTIFICATION OF BUSINESS PARTNERS
The Contractor shall identify all of its business partners and subcontractors related to services provided. under this contract, who will be involved in any application development and/or operations.

45. LOCATION OF END USER DATA
All State data hosted by the contractor will be stored in facilities located in the United States of America. At no time is it acceptable for any State data to be stored in facilities outside the United States of America. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the United States of America.

46. HANDLING OF DATA BREACHES
The Vendor will implement, maintain and update security incident and data breach procedures that comply with all State and Federal requirements. Immediately upon becoming aware of the possibility of a data breach, the Vendor will notify the State. A data breach is the disclosure of unauthorized access to, use of, modification of, or destruction of State data or the interference with system operations in an information system containing State data. The Vendor will also (i) fully investigate the incident, (ii) cooperate fully with the State's investigation of, analysis of, and response to the incident, (iii.) promptly implement necessary remedial measures and (iv) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services. The Vendor will use a credit monitoring service, forensics company, advisors, public relations firm and legal counsel that are acceptable to the State, preserve all evidence including but not limited to communications, documents, and logs and the State will have the authority to set the scope of the investigation. In addition, the Vendor shall inform the State of the actions it is taking or will take to reduce the risk of further loss to the State.

Except as otherwise required by law, the Vendor shall only provide notice of the incident to the State. The State will determine whether notification to the affected parties will; (i) jeopardize the State's interests and (ii) be more appropriate for the Vendor to provide notification.   The method and content of the notification of the affected parties must be coordinated with and is subject to approval by the State. If the Vendor is required by federal law or regulation to conduct a security incident or data breach investigation the results of the investigation must be reported to the State. If the Vendor is required by federal law or regulation to notify the affected parties State must also be notified.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in investigation and remediation of such data breach, including but not limited to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract. The Vendor shall also reimburse the State in full for all costs the State incurs in its offering of 2 years credit monitoring to each person whose data were compromised. The Vendor shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the data breach.

47. SECURITY BREACHES AND BREACH RESPONSIBILITIES
The Vendor, unless stipulated otherwise, shall notify the State Contact within ______ if the Vendor reasonably believes there has been a security incident.

If notification of a security incident or data breach to the State Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within twelve (12) hours after law-enforcement provides permission for the release of information on the security incident or data breach.

Notification to the State should include at a minimum, (i) Name of and contact information for the Vendor's Point of Contact for the security incident or data breach, (ii) date and time of the security incident or data breach; (iii) date and time the security incident or data breach was discovered, (iv) description of the security incident or data breach including the data involved, being as specific as possible, (v) potential number of records known and if unknown the range of records, (vi) address where the security incident or data breach occurred, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via federally approved encryption techniques. If there are none, the encryption levels specified in paragraph 37 should be used. Vendor shall use the term "data incident report" in the subject line of the email. If all of the information is not available for the notification within the specified period of time, Vendor shall provide the state with all of the available information.

48. CYBER LIABILITY INSURANCE
The Vendor shall maintain cyber liability insurance with liability limits in the amount of $________ to protect any and all State data the Vendor receives as part of the project covered by this agreement including State data that may reside on devices, including laptops and smart phones, utilized by Vendor employees, whether the device is owned by the employee or the Vendor. If the Vendor has a contract with a third-party to host any State data the Vendor receives as part of the project under this agreement, then the Vendor shall include a requirement for cyber liability insurance as part of the contract between the Vendor and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include state data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-part vendor. The cyber liability insurance shall cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Vendor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Vendor shall furnish copies of insurance policies if requested by the State.

49. CHANGE MANAGEMENT PROCESS
From time to time it may be necessary or desirable for either the State or the Vendor to propose changes in the Services provided. Such changes shall be effective only if they are in writing and contain the dated signatures of authorized representatives of both parties. Unless otherwise indicated, a change or amendment shall be effective on the date it is signed by both parties. Automatic upgrades to any software used by the Vendor to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by the Vendor on a schedule no less favorable than that provided by the Vendor to any other customer receiving comparable levels of services.

50. BROWSER
The system, site, and/or application must be compatible with the State's current browser standard which can be found at, http://bit.sd.gov/standards/. Neither PHP nor Adobe ColdFusion will be used in the system, site, and/or application.

51. SECURITY ACKNOWLEDGEMENT FORM

The Vendor employees and any subcontractor(s') as well as the subcontractor(s') employees, participating in the work covered by this Agreement will be required to sign the Security Acknowledgement form which is attached to this Contract as Attachment C. The signed Security Acknowledgement form(s) must be given to the State and approved by BIT before work on the contract may begin. This form commits the Vendor to abide by the terms of the Information Technology User's Security Guide (ITUSG). Failure to abide by the requirements of the ITUSG or the Security Acknowledgement form is a breach of this Agreement. It is also a breach of this Agreement if the Vendor does not obtain the signature on the Security Acknowledgement from any employees and any subcontractor(s') as well as the subcontractor(s') employees, any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Vendor's or subcontractor's employees due to a failure of an employee to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Vendor or Subcontractor and in accordance with the Vendor's or Subcontractor's personnel policies. Regardless of the actions taken by the Vendor or Subcontractor, the State shall retain the right to require at its discretion the removal of the employee from the project covered by this agreement.

52. BACKGROUND CHECKS

The State of South Dakota requires all employee(s) of the Vendor, subcontractor(s) and or agent(s) who write or modify State of South Dakota-owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected-personally identifiable information or have access to secure areas to have fingerprint-based background checks. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the finger print cards and the procedure that is to be used to process the finger print cards. Project plans should allow two to four weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Vendor, subcontractor(s) and or agent(s) will be writing or modifying State of South Dakota-owned software, altering hardware, configuring software of state-owned technology resources, have access to source code and/or protected-personally identifiable information or have access to secure areas then background checks must be performed on any employees who will complete any of the referenced tasks.

53. SECURITY

The Vendor shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks.

By signing this agreement, the Vendor warrants that:

A. All known security issues are resolved.

B. Assistance will be provided to the State by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. This investigation can include security scans made at the State's discretion. Failure by the Vendor to remedy any security issues discovered can be considered a breach of this agreement by the State.

54. PERFORMANCE OF ADDITIONAL WORK

The Vendor will perform additional work on their application at the hourly rate of $ ________. This work can be authorized by any of the State signatories to this agreement. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third party technologies or excessive resource consumption. Completion of this additional work can be a requirement for an application to go into or stay in production.

55. AUTHORIZED SIGNATURES**:**
In witness hereto, the parties signify their agreement by affixing their signatures hereto.

Consultant Signature ______________________________ Date ______________

State - DSS Division Director Carrie Johnson ______________________________ Date ______________

State - DSS Deputy Secretary Brenda Tidball-Zeltinger ______________________________ Date ______________

State – DSS Cabinet Secretary Lynne A. Valenti ______________________________ Date ______________

State – Bureau of Information and Telecommunications Commissioner
David Zolnowsky ______________________________ Date ______________

State Agency Coding:

CFDA #				
Company				
Account				
Center Req				
Center User				
Dollar Total				

DSS Program Contact Person ______________________________
Phone ______________

DSS Fiscal Contact Person Patty Hanson
Phone 605 773-3586

Consultant Program Contact Person ______________________________
Phone ______________

Consultant Fiscal Contact Person ______________________________
Phone ______________________________
Consultant Email Address ______________________________

SDCL 1-24A-1 states that a copy of all consulting contracts shall be filed by the State agency with the State Auditor within five days after such contract is entered into and finally approved by the contracting parties. For further information about consulting contracts, see the State Auditor's policy handbook.

Attachment B

Security and Vendor Questions

A = Data Center
B = Development
C = PMO Office
D = Telecommunications

	BIT Owner	Question	Response	Add text as required
1.	C	**Typically the State of South Dakota prefers to host all systems. In the event that the State decides that it would be preferable for the vendor to host the system, is this an option?**	**Yes☐ No☐ NA ☐**	
2.	D	Is there a workstation install requirement?	Yes☐ No☐ NA ☐	
3.	A/D	Is this a browser based User Interface?	Yes☐ No☐ NA ☐	
4.	B/C	What is the development technologies used for this system? ASP ___________ VB.Net ___________ C#.Net ___________ .NET Framework ___________ Java/JSP ___________ MS SQL ___________		
5.	A	Will the system support authentication?	Yes☐ No☐ NA ☐	
6.	A	Will the system infrastructure require an email interface?	Yes☐ No☐ NA ☐	
7.	A	Will the system require a database?	Yes☐ No☐ NA ☐	
8.	A	Will the system infrastructure require database replication?	Yes☐ No☐ NA ☐	
9.	A	Will the system require transaction logging for database recovery?	Yes☐ No☐ NA ☐	

10.	A	Will the system infrastructure have a special backup requirement?	Yes☐ No☐ NA ☐	
11.	B/C	Will the system provide an archival solution? If not is the State expected to develop a customized archival solution?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
12.	A	Will the system infrastructure have any processes that require scheduling?	Yes☐ No☐ NA ☐	
13.	A/B	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?	Yes☐ No☐ NA ☐	
14.	A/B	Will the system infrastructure require a Business Intelligence solution?	Yes☐ No☐ NA ☐	
15.	B/C	Will the system have any workflow requirements?	Yes☐ No☐ NA ☐	
16.	C	Explain the software licensing model.		
17.	A	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?	Yes☐ No☐ NA ☐	
18.	A	Can the system be implemented via Citrix?	Yes☐ No☐ NA ☐	
19.	B/D	Will the system implement its own level of security?	Yes☐ No☐ NA ☐	
20.	A	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?	Yes☐ No☐ NA ☐	
21.	A	Will the system print to a Citrix compatible networked printer?	Yes☐ No☐ NA ☐	
22.	D	Will the network communications meet IEEE standard TCP/IP and use either standard ports or State defined ports as the State determines?	Yes☐ No☐ NA ☐	
23.	A/D	Will the system provide Internet security functionality on Public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?	Yes☐ No☐ NA ☐	
24.	D	Will the system provide Internet security functionality on a public portal to include firewalls?	Yes☐ No☐ NA ☐	
25.	D	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies, would this affect the implementation of the system?	Yes☐ No☐ NA ☐	

26.	D	Does your application use Java, is it locked into a certain version or will it use the latest version if so what is your process for updating the application?	Yes☐ No☐ NA ☐	
27.	D	If your application does not run under the latest Microsoft operating system what is your process for updating the application?		
28.	A	Will the server based software support: a. Windows server 2012 R2 b. IIS7.0 or higher c. MS SQL Server 2008R2 or higher d. Exchange 2010 or higher e. Citrix presentation server 4.5 or higher f. VMWare ESXi 5.5 or higher g. MS Windows Updates h. Symantec End Point Protection	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
29.	B	Identify each of the Data, Business and Presentation layer technologies your product would use and provide a roadmap outlining how your release and or update roadmap aligns with the release and or update roadmap for this technology.		
30.	D	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, IDS/IPS and desktop security infrastructure. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
31.	A	It is State policy that all systems must be compatible with BITs dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
32.	A	It is State policy that all systems that require an email interface must leverage existing SMTP processes currently managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
33.	D	It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Secure Gateway. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	

34.	D	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
35.	A	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. If need is determined by the State, would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
36.	A	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
37.	D	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
38.	D	It is State policy that systems must support NAT and PAT running inside the State Network. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
39.	D	It is State policy that systems must not use dynamic TCP or UDP ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
40.	D	Will your system use Adobe Air, Adobe Flash, Apache Flex, JavaFX , Microsoft Silverlight? If yes what are your plans for moving off them?	Yes☐ No☐ NA ☐	
41.	D	Does your web application use PHP or Adobe ColdFusion?	Yes☐ No☐ NA ☐	
42.	A/B	How does data enter the system (transactional or batch or both)?		
43.	C	Is the system data exportable by the user for use in tools like Excel or Access?	Yes☐ No☐ NA ☐	
44.	C	Will user customizable data elements be exportable also?	Yes☐ No☐ NA ☐	
45.	C	Will the system distinguish between local versus global administrators where local administrators have rights to user management only for the program area that they are associated with and global administrators have rights for the entire system?	Yes☐ No☐ NA ☐	

46.	C	Will this system provide the capability to track data entry/access by the person, date and time?	Yes☐ No☐ NA ☐	
47.	A/B/ C/D	Will the system provide data encryption for sensitive information both in storage and transmission?	Yes☐ No☐ NA ☐	
48.	D	It is State policy that systems at the discretion of the State may have a Security Audit performed on it by BIT or a 3rd Party for security vulnerabilities. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
49.	C/D	The Vendors/Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the state's discretion a vendor's answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the vendor selection criteria. Is this acceptable?	Yes☐ No☐ NA ☐	
50.	A	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?	Yes☐ No☐ NA ☐	
51.	A/C	Will the vendor provide assistance with installation?	Yes☐ No☐ NA ☐	
52.	A/C	Is there an installation guide available and will you provide a copy to the State?	Yes☐ No☐ NA ☐	
53.	A/C	Is telephone assistance available for both installation and use?	Yes☐ No☐ NA ☐	
54.	A/B /C	Is on-site assistance available? If so, is there a charge?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
55.	A/B /C	Will the implementation plan include user acceptance testing?	Yes☐ No☐ NA ☐	
56.	B	Will technical documentation for application maintenance purposes be provided to the State?	Yes☐ No☐ NA ☐	
57.	B/C	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?	Yes☐ No☐ NA ☐	
58.	C	Can the user manual be printed?	Yes☐ No☐ NA ☐	
59.	C	Is the user manual electronically available?	Yes☐ No☐ NA ☐	

60.	C	Is there on-line help assistance available?	Yes☐ No☐ NA ☐	
61.	C	Describe your Support options.		
62.	A/C	Is there a method established to communicate availability of system updates?	Yes☐ No☐ NA ☐	
63.	A/D	The State implements enterprise wide anti-virus solutions on all servers and workstations as well as controls the roll-outs of any and all Microsoft patches based on level of criticality. Do you have any concerns in regards to this process?	Yes☐ No☐ NA ☐	
64.	B/C	Will you provide customization of the system if required by the State of South Dakota?	Yes☐ No☐ NA ☐	
65.	B	Will the state be required to develop customized interfaces to other applications?	Yes☐ No☐ NA ☐	
66.	B	Will the State be required to develop reports or data extractions from the database?	Yes☐ No☐ NA ☐	
67.	A/B /C	Will the State of South Dakota have access to the underlying data and data model for ad hoc reporting purposes?	Yes☐ No☐ NA ☐	
68.	C	Will the source code for the system be put in escrow for the State of South Dakota?	Yes☐ No☐ NA ☐	
69.	C	If the source code is placed in escrow, will the vendor pay the associated escrow fees?	Yes☐ No☐ NA ☐	
70.	B/C	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?	Yes☐ No☐ NA ☐	
71.	C	Explain the basis on which pricing could change for the state based on your licensing model.		
72.	C	Contractually, how many years price lock are you offering the state as part of your response? Also as part of your response, how many additional years are you offering to limit price increases and by what percent?		
73.	B/C	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?	Yes☐ No☐ NA ☐	
74.	B/C	Has your company ever conducted a project where you were tasked with performing load testing?	Yes☐ No☐ NA ☐	
75.	B/C	Has your company ever developed a system that ran on Citrix Metaframe?	Yes☐ No☐ NA ☐	
76.	B/C	Have you ever created a User Acceptance Test plan and test cases?	Yes☐ No☐ NA ☐	

77.	C	It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Secure Gateway. Would this affect the implementation of the system? If the policy above is not acceptable, will your proposed VPN Connections meet the following requirements: o Pre-Shared Key o AES (256bits or Higher) o SHA1 o No PFS or Aggressive Modes allowed.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
78.	C	Are there expected periods of time where the application will be unavailable for use?	Yes☐ No☐ NA ☐	
79.	C	Is there a strategy for mitigating unplanned disruptions?	Yes☐ No☐ NA ☐	
80.	C	Will the State of South Dakota own the data created in your hosting environment?	Yes☐ No☐ NA ☐	
81.	C	Will the State acquire the data at contract conclusion?	Yes☐ No☐ NA ☐	
82.	C	Will organizations other than the State of South Dakota have access to our data?	Yes☐ No☐ NA ☐	
83.	C	Will the State's data be used for any other purposes other than South Dakota's usage?	Yes☐ No☐ NA ☐	
84.	C	Will the State's data be protected?	Yes☐ No☐ NA ☐	
85.	C	List any hardware or software you propose to use that is not state standard, the standards can be found at http://bit.sd.gov/standards/.		
86.	A	Please explain the pedigree of the software, include in your answer who are the people, organization and processes that created the software		
87.	A	Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure.		
88.	D	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components	Yes☐ No☐ NA ☐	

		are used during the development process? Provide a brief explanation. Will the supplier indemnify the Acquirer from these issues in the license agreement? Provide a brief explanation.	Yes☐ No☐ NA ☐	
89.	B	What are the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software (brief summary response)?		
90.	B	Explain what form of software assurance is used in development?		
91.	D	Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.		
92.	D	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?	Yes☐ No☐ NA ☐	
93.	B	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?	Yes☐ No☐ NA ☐	
94.	B	Are there some requirements for security that are “structured” as part of general releasability of a product and others that are “as needed” or “custom” for a particular release?	Yes☐ No☐ NA ☐	
95.	D	What process is utilized by your company to prioritize security related enhancement requests?		
96.	D	What threat assumptions were made, if any, when designing protections for the software and information assets processed?		
97.	B	What security design and security architecture documents are prepared as part of the SDLC process?		
98.	D	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?	Yes☐ No☐ NA ☐	
99.	A	Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before being used.		
100.	D	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user) and is it designed to isolate and minimize the extent of damage possible by a successful attack?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

101.	D	Where applicable, does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?	Yes☐ No☐ NA ☐	
102.	D	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?		
103.	D	What security criteria, if any, are considered when selecting third-party suppliers?		
104.	B	What coding and/or API standards are used during development of the software?		
105.	B	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, integrated testing)?		
106.	D	Who and when are security tests performed on the product? Are tests performed by an internal test team, by an independent third party, or by both?		
107.	B	Are misuse test cases included to exercise potential abuse scenarios of the software?	Yes☐ No☐ NA ☐	
108.	B	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?	Yes☐ No☐ NA ☐	
109.	D	What release criteria does your company have for its products with regard to security?		
110.	B	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?		
111.	B	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?		
112.	D	How has the software been measured/assessed for its resistance to identified, relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs) used? How have the findings been mitigated?		
113.	D	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If the CC, what evaluation assurance level (EAL) was achieved? If the product claims conformance to a protection profile, which one(s)? Are the security target and evaluation report available?	Yes☐ No☐ NA ☐	

114.	A/D	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
115.	A/B	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
116.	A/D	Has the product undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
117.	B	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)? If yes please explain.	Yes☐ No☐ NA ☐	
118.	A/B	Is there a Support Lifecycle Policy within the organization for the software in question? Does it outline and establish a consistent and predictable support timeline?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
119.	A	How will patches and/or Service Packs be distributed to the Acquirer?		
120.	B	What services does the help desk, support center, or (if applicable) online support system offer?		
121.	A/B	How extensively are patches and Service Packs tested before they are released?		
122.	A	Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack automated or manual?	Yes☐ No☐ NA ☐	
123.	A/B	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?		
124.	A	How do you set the relative severity of defects and how do you prioritize their remediation?		

125.	A	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?		
126.	A	Are third-party developers contractually required to follow your configuration management policies?	Yes☐ No☐ NA ☐	
127.	B	What policies and processes does your company use to verify that software components do not contain unintended, "dead," or malicious code? What tools are used?		
128.	B	How is the software provenance verified (e.g. any checksums or signatures)?		
129.	A	Does your company publish a security section on its Web site? If so, do security researchers have the ability to report security issues?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
130.	A	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?	Yes☐ No☐ NA ☐	
131.	A	Has your company ever filed for Recompany under U.S. Code Chapter 11? If so, please provide dates for each incident and describe the outcome.	Yes☐ No☐ NA ☐	
132.	A	Are security requirements developed independently of the rest of the requirements engineering activities, or are they integrated into the mainstream requirements activities?		
133.	A/B /D	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?		
134.	B	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.	Yes☐ No☐ NA ☐	
135.	B	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?	Yes☐ No☐ NA ☐	
136.	A	Does the organization ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of "trigger" events.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
137.	B	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?	Yes☐ No☐ NA ☐	

138.	B	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user) and is it designed to isolate and minimize the extent of damage possible by a successful attack?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
139.	B	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?		
140.	B	Does the exception-handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
141.	B	Does the documentation explain how to install, configure, and/or use the software securely? Does it identify options that should not normally be used because they create security weaknesses?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
142.	B	Where applicable, does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?	Yes☐ No☐ NA ☐	
143.	B	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?		
144.	A	Does the software have any security critical dependencies or need additional controls from other software (e.g., operating system, directory service, application), firmware, or hardware? If yes, please describe.	Yes☐ No☐ NA ☐	
145.	A	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?		
146.	B	What types of functional tests are performed on the software during its development (e.g., spot checking, component-level testing, security testing, integrated testing)?		
147.	A	Does your company's defect classification scheme include security categories?	Yes☐ No☐ NA ☐	
148.	B	What percentage of code coverage does your testing provide?		
149.	B	Are misuse test cases included to exercise potential abuse scenarios of the software?	Yes☐ No☐ NA ☐	
150.	A	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?	Yes☐ No☐ NA ☐	

151.	B	When does security testing occur during the SDLC (e.g., unit level, subsystem, system, certification and accreditation)?		
152.	A	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation?	Yes☐ No☐ NA ☐	
153.	B	Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
154.	B	Are static or dynamic software security analysis tools used to identify the weaknesses that can lead to exploitable vulnerabilities in the software? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
155.	B	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
156.	B	How is the assurance of software produced by third-party developers assessed?		
157.	A	How will patches and/or Service Packs be distributed to the Acquirer?		
158.	D	How are trouble tickets submitted? How are support issues, specifically those that are security related, escalated?		
159.	A	Are help desk or support center personnel internal company resources or are these services outsourced to third parties?		
160.	A	If help desk or support center services are outsourced to third parties, are they located in foreign countries?		
161.	B	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?		
162.	B	What policies and processes does your organization use to verify that software components do not contain unintended, “dead,” or malicious code? What tools are used?		
163.	B	Does your company have a vulnerability management and reporting policy? Is it available for review?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
164.	A	Does your company perform background checks on members of the software development team? If so, are there any additional “vetting” checks done on people who work on critical application components, such as security? Explain.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

165.	B	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle, explain.	Yes☐ No☒ NA ☐	
166.	A	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.	Yes☐ No☐ NA ☐	
167.	A	Please summarize your company's history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).		
168.	A	Is the controlling share (51+%) of your company owned by one or more non-U.S. entities?	Yes☐ No☐ NA ☐	
169.	A	What are your customer confidentiality policies? How are they enforced?		
170.	D	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?		
171.	A	What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same host server?		
172.	A	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?	Yes☐ No☐ NA ☐	
173.	A	What are your policies and procedures for hardening servers?		
174.	A	What are your data backup policies and procedures? How frequently are your backup procedures verified?		
175.	A	What are the procedures for evaluating any vendor security alerts and installing patches and Service Packs?		
176.	A	Is testing done after changes are made to servers? What are your rollback procedures in the event of problems resulting from installing a patch or Service Pack?	Yes☐ No☐ NA ☐	
177.	A	If you have agents or scripts executing on servers of hosted applications and what are the procedures for reviewing the security of these scripts or agents?		

178.	A	What are the procedures and policies used to control access to the servers? Are audit logs maintained?		
179.	A	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?		
180.	A	Do you have a formal disaster recovery plan? What actions will be taken to recover from a disaster? Are warm or hot backups available?	Yes☐ No☐ NA ☐	
181.	A	Is two-factor authentication used for administrative control of all security devices and critical information systems?	Yes☐ No☐ NA ☐	
182.	A/D	How are virus prevention, detection, correction, and updates handled for the products?		
183.	D	What type of firewalls (or application gateways) do you use? How are they monitored/managed?		
184.	D	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?		
185.	A/D	Explain or provide a diagram of the architecture for the application including security mitigation.		
186.	A	Do you perform regular reviews of system and network logs for security issues?	Yes☐ No☐ NA ☐	
187.	A	Do you have an automated security event management system?	Yes☐ No☐ NA ☐	
188.	A	What are your procedures for intrusion detection, incident response, and incident investigation/escalation?		
189.	A	Will you provide on-site support 24x7 to resolve security incidents?	Yes☐ No☐ NA ☐	
190.	A	Are security logs and audit trails protected from tampering or modification?	Yes☐ No☐ NA ☐	
191.	A	How do you control physical and electronic access to the log files? Are log files consolidated to single servers?		
192.	A	Do you provide security performance measures to the customer at regular intervals?	Yes☐ No☐ NA ☐	
193.	A	Describe your security testing processes.		
194.	A	Do you perform penetration testing of the service? If yes, how frequently are penetration tests performed? Are the tests performed by internal resources or by a	Yes☐ No☐ NA ☐	

		third party?		
195.	A	How frequently is the security tests performed? Are the tests performed by internal resources or by a third party?		
196.	A	Do you have a SOC 2 audit report? Is the audit done annually? Does the audit cover all 5 of the trust principles? Does the audit include subservice providers? Has the auditor ever been unable to attest to an acceptable audit result? Will you provide a copy of your latest SOC 2 audit upon request, a redacted version is acceptable.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
197.	A	Are you or if the data is being hosted by a subservice provider are they FedRAMP certified?	Yes☐ No☐ NA ☐	
198.	B	Do you use open source software or libraries? If yes do you check for vulnerabilities in your software or library that are listed in: a. Common Vulnerabilities and Exposures (CVE) database? b. Open Source Vulnerability Database (OSVDB)? c. Open Web Application Security Project (OWASP) Top Ten?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

Attachment C

BIT: Security Acknowledgement

Please return requests to your Manager

Following is the Employee Agreement that all BIT employees and State contractors must sign; **Employee Agreement to Comply with BIT Technology Infrastructure Security Policy.** The State of South Dakota is dedicated to information security and has security specialists in each BIT Division. However, users are responsible for compliance to all information security policies and procedures. *<u>By signature below, the employee / contractor hereby acknowledges and agrees to the following:</u>*

1. Employee or contractor is a “user” as defined in the State of South Dakota BIT: ITUSG;
2. Employee is a State of South Dakota employee or contractor that uses State of South Dakota technology infrastructure or information;
3. Employee / contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;
4. Employee / contractor has read and agrees to abide by the State of South Dakota BIT: ITUSG;
5. Employee / contractor consents to discuss with a supervisor / State contact regarding policies or procedures not understood within the BIT: ITUSG;
6. Employee / contractor shall abide by the policies described as a condition of continued employment / service;
7. Employee / contractor understands that any individual found to violate the BIT: ITUSG is subject to disciplinary action, including but not limited to, privilege revocation, employment termination and financial reimbursement;
8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;
9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment;
10. Employee / contractor shall promptly report violations of BIT: ITUSG policies to a manager / State contact and BIT Help Desk;
11. This document may be amended from time to time. The State of South Dakota recommends employees for the State to regularly review the BIT: ITUSG, and annual amendments on the State of South Dakota Intranet. http://intranet.bit.sd.gov/policies/docs/BIT-Security%20Information%20Technology%20User%20Security%20Guide.pdf

ACKNOWLEDGMENT: STATE OF SOUTH DAKOTA INFORMATION TECHNOLOGY SECURITY GUIDE

Employee / contractor signature **Date** **Manager\ State contact** **Date**

Employee / contractor name in block capital letters